# On a Class of Majority-Logic Decodable Cyclic Codes

JEAN-MARIE GOETHALS AND PHILIPPE DELSARTE

***Abstract*—A new infinite class of cyclic codes is studied. Codes of this class can be decoded in a step-by-step manner, using majority logic. Some previously known codes fall in this class, and thus admit simpler decoding procedures. As random error-correcting codes, the codes are nearly as powerful as the Bose–Chaudhuri codes.**

## I. INTRODUCTION

A NEW infinite class of cyclic codes is studied, which has the interesting property that majority-logic decoding can be used in a step-by-step manner as in Meggitt's[10] general decoder. The class contains as a proper subclass the difference-set cyclic codes, introduced by Weldon.[3] Also, the Reed–Muller codes,[5],[6] with one coordinate place removed, fall in this class. Finally, some Bose–Chaudhuri codes[11] fall in this class, and are therefore more simply decoded. The codes are defined as orthogonal on some tactical configurations in projective geometries.

Some properties of finite projective geometries are first recalled in order to make the paper relatively self-contained. The dimension of the codes is then derived, implying Graham and MacWilliam's result.[4] Decoding and implementation of the codes are discussed.

## II. PROPERTIES OF CONFIGURATIONS DEDUCED FROM FINITE PROJECTIVE GEOMETRIES

For the sake of completeness, let us first recall here a number of properties of finite geometries.[1]

Let $GF(q)$ be the Galois field with $q$ elements, where $q$ is some power of a prime, say $q = p^n$. Then, $GF(q^{m+1})$ can be represented as an algebra of dimension $(m + 1)$ over $GF(q)$, and the points of the $m$-dimensional finite projective geometry $PG(m, q)$ can be represented as the $(q^{m+1} - 1)/(q - 1)$ distinct subspaces of dimension 1 over $GF(q)$. Two elements $\alpha$ and $\beta$ of $GF(q^{m+1})$ such that $\beta = \lambda\alpha$, where $\lambda$ belongs to $GF(q)$, represent thus the same point of the $PG(m, q)$. A $PG(s, q)$, with $s < m$, contained in the $PG(m, q)$ is defined as the set of points of $PG(m, q)$ which are on the same $(s + 1)$-dimensional subspace over $GF(q)$. It is thus defined by $(s + 1)$ linearly independent points, and there are

$$b(s, m, q) = \frac{(q^{m+1} - 1)(q^m - 1) \cdots (q^{m-s+1} - 1)}{(q^{s+1} - 1)(q^s - 1) \cdots (q - 1)} \tag{1}$$

distinct $PG(s, q)$ contained in a given $PG(m, q)$. Furthermore, a given $PG(t, q)$ with $t < s < m$, is contained in exactly

$$\lambda(t, s, m, q) = \frac{(q^{m-t} - 1)(q^{m-t-1} - 1) \cdots (q^{m-s+1} - 1)}{(q^{s-t} - 1)(q^{s-t-1} - 1) \cdots (q - 1)} \tag{2}$$

distinct $PG(s, q)$ which are contained in a given $PG(m, q)$. One easily deduces that the incidence relations of the $b(s, m, q)$ distinct $PG(s, q)$ on the points of a given $PG(m, q)$ define a balanced incomplete block design[1] with parameters

$$\begin{aligned} v &= (q^{m+1} - 1)/(q - 1) \\ k &= (q^{s+1} - 1)/(q - 1) \\ b &= b(s, m, q) \\ r &= \lambda(0, s, m, q) \\ \lambda &= \lambda(1, s, m, q) \text{ for } s > 1, \quad \text{and } \lambda = 1, \quad \text{for } s = 1. \end{aligned} \tag{3}$$

We are interested in the linear subspace over $GF(p)$ generated by the $b$ rows of the incidence matrix of that configuration. We first give a concrete representation of that configuration.

Let $\alpha$ be a primitive root in $GF(q^{m+1})$. Then, $\beta = \alpha^{(q-1)}$ is a primitive $v$th root of unity, and $\omega = \alpha^v$ is a primitive root in $GF(q)$. We can and do represent the points of $PG(m, q)$ by the first $v$ distinct powers of $\alpha$, since

$$\alpha^{d_1} = \omega^i \alpha^{d_2}$$

is impossible if $d_1$ and $d_2$ are both less than $v$. Let $\alpha^{d_0}$, $\alpha^{d_1}, \cdots, \alpha^{d_s}$ be $s + 1$ points of $PG(m, q)$ which are linearly independent over $GF(q)$, and consider the $(q^{s+1} - 1)/(q - 1)$ nonzero linear combinations

$$\sum_{j=0}^{s} \lambda_{ij}\alpha^{d_j} = c_i \tag{4}$$

of these points, where the $\lambda_{ij}$ belonging to $GF(q)$ are such that no two vectors $\lambda_i = (\lambda_{i0}, \lambda_{i1}, \cdots, \lambda_{is})$ are dependent over $GF(q)$. The $c_i$ so obtained are elements of $GF(q^{m+1})$ and can be expressed in the form

$$c_i = \omega^{h_i}\alpha^{d_i}, \tag{5}$$

where $d_i$ is less than $v$; furthermore, no two $d_i$ are equal since otherwise the corresponding vectors $\lambda_i$ would be dependent over $GF(q)$. We thus can and do take the $k = (q^{s+1} - 1)/(q - 1)$ points $\alpha^{d_i}$ as the elements of a

---

Manuscript received April 20, 1967. This paper was presented at the 1967 International Symposium on Information Theory, San Remo, Italy.

The authors are with the Manufacture Belge de Lampes et de Materiel Electronique (MBLE), Brussels, Belgium.

[1] The interested reader may consult Mann[9] or Carmichael.[7]

$PG(s, q)$ contained in $PG(m, q)$. The polynomial

$$w(x) = x^{d_0} + x^{d_1} + \cdots + x^{d_{k-1}}, \tag{6}$$

which we take as an element of the algebra of polynomials modulo $(x^v - 1)$ over $GF(p)$, will then represent a row in the incidence matrix. Taking all possible sets of $(s + 1)$ linearly independent points will give the $b$ distinct rows.

We note that the linear subspace generated by these vectors is cyclic. For, if $w(x)$ is a vector of the incidence matrix, so is $x\ w(x)$, since (4) and (5) imply

$$\alpha c_i = \omega^{h_i} \alpha^{d_i + 1} = \sum_{j=0}^{s} \lambda_{ij} \alpha^{d_j + 1}.$$

Thus, as shown by Peterson,[1] this cyclic subspace is an ideal in the algebra of polynomials modulo $(x^v - 1)$ and its dimension over $GF(p)$ is $v - h$, if $h$ is the number of $v$th roots of unity that are roots of all polynomials $w(x)$. The next section will be devoted to the determination of this number $h$.

## III. DIMENSION OVER $GF(p)$ OF THE CODES $C(s, m, p^n)$

Let us denote by $C(s, m, q)$ the cylic code generated over $GF(p)$ by the set of polynomials $w(x)$ (6). To determine the dimension of this code is equivalent to finding the number of $v$th roots of unity that are roots of all polynomials $w(x)$.

It is the purpose of this section to prove the following proposition, where $u$ stands for $q - 1 = p^n - 1$.

*Theorem 1*

The number of $v$th roots of unity that are roots of all polynomials $w(x)$ is the number of integers $t$, less than or equal to $v$, $t \neq 0$, such that all multinomial coefficients

$$\frac{(tu)!}{(l_0 u)!\,(l_1 u)! \cdots (l_s u)!}, \quad l_i \neq 0,$$

$$l_0 + l_1 + \cdots + l_s = t$$

are congruent to zero mod $p$.

Several preliminary steps are needed. If $\alpha$ is a primitive root in $GF(q^{m+1})$, then $\beta = \alpha^u$ is a primitive $v$th root of unity. With $w(x)$ defined in (6), let us write

$$w(\beta^t) = \sum_{i=0}^{k-1} \alpha^{utd_i}, \tag{7}$$

which, using (4), (5), and $\omega^u = 1$, becomes

$$w(\beta^t) = \sum_{i=0}^{k-1} \left( \sum_{j=0}^{s} \lambda_{ij} \alpha^{d_j} \right)^{ut}, \tag{8}$$

where the right-hand member is a function of the $\alpha^{d_i}$ which we denote by

$$F_{s,t}(\alpha_0, \alpha_1, \cdots, \alpha_s),$$

where $\boldsymbol{\alpha_i}$ stands for $\alpha^{d_i}$. That this function is symmetric with respect to the $\alpha_i$ is easily shown, since the sum

$$w(\beta^t) + w(\omega\beta^t) + \cdots + w(\omega^{q-2}\beta^t), \tag{9}$$

which equals $(q - 1)F_{s,t}(\alpha_0, \alpha_1, \cdots, \alpha_s)$, can be exhibited as

$$\sum_{\mu_0, \mu_1, \mu_2, \cdots, \mu_s} (\mu_0\alpha_0 + \mu_1\alpha_1 + \cdots \mu_s\alpha_s)^{ut}, \tag{10}$$

where $\mu_0, \mu_1, \cdots, \mu_s$ each run through the $q$ elements of $GF(q)$.

*Lemma 1*

$$F_{s,t}(\alpha_0, \alpha_1, \cdots, \alpha_s)$$

$$= (-1)^s \sum_{l_0, l1, \cdots, l_s} \frac{(tu)!}{(l_0 u)!\,(l_1 u)! \cdots (l_s u)!} \alpha_0^{l_0 u} \alpha_1^{l_1 u} \cdots \alpha_s^{l_s u} \pmod p,$$

where $l_i \neq 0$, and $l_0 + l_1 + \cdots + l_s = t$.

*Proof*: According to (10), one may write

$$(q - 1)F_{s,t}(\alpha_0, \alpha_1, \cdots \alpha_s)$$

$$= \sum_{\mu_1, \mu_2, \cdots, \mu_s} \sum_{\mu_0} [\mu_0\alpha_0 + (\mu_1\alpha_1 + \cdots + \mu_s\alpha_s)]^{ut}.$$

Now, expanding the term under brackets

$$(\mu_0\alpha_0 + x)^{ut} = x^{ut} + \sum_{i=1}^{ut} \binom{ut}{i} \mu_0^i \alpha_0^i x^{ut-i},$$

where $x$ stands for $(\mu_1\alpha_1 + \cdots + \mu_s\alpha_s)$, and summing in $\mu_0$ over all elements of $GF(q)$, one obtains

$$(q - 1)F_{s,t}$$

$$= \sum_{\mu_1, \mu_2, \cdots, \mu_s} \left[ qx^{ut} + \sum_{i=1}^{ut} \binom{ut}{i} \alpha_0^i x^{ut-i} \left( \sum_{\mu_0} \mu_0^i \right) \right]. \tag{11}$$

Now, the sum

$$\sum_{\mu_0} \mu_0^i$$

equals $(q - 1)$ when $i$ is a multiple of $u = q - 1$, and is zero otherwise, so that (11) becomes modulo $p$,

$$F_{s,t} = \sum_{\mu_1, \mu_2, \cdots, \mu_s} \sum_{l=1}^{t} \binom{ut}{ul} \alpha_0^{ul} (\mu_1\alpha_1 + \mu_2\alpha_2 + \cdots + \mu_s\alpha_s)^{(t-l)u}. \tag{12}$$

But, for $l = t$, the sum in $\mu_1, \mu_2, \cdots, \mu_s$ gives $q^s$ times $\alpha_0^{ut}$, which is zero mod $p$; on the other hand, one may write

$$\sum_{\mu_1, \mu_2, \cdots, \mu_s} (\mu_1\alpha_1 + \mu_2\alpha_2 + \cdots + \mu_s\alpha_s)^{(t-l)u}$$

$$= -F_{s-1, t-l}(\alpha_1, \alpha_2, \cdots, \alpha_s),$$

so that (12) becomes

$$F_{s,t} = \sum_{l=1}^{t-1} \binom{ut}{ul} \alpha_0^{ul} [-F_{s-1, t-l}(\alpha_1, \alpha_2, \cdots, \alpha_s)]. \tag{13}$$

By induction, one obtains the desired result.

*Lemma 2*

$\boldsymbol{F_{s,t}}(\alpha_0, \alpha_1, \cdots, \alpha_s)$ is equal to zero if the elements $\alpha_0, \alpha_1, \cdots, \alpha_s$ are linearly dependent over $GF(q)$.

*Proof*: First, as previously shown, one can write

$$(q-1)F_{s,t}(\alpha_0, \alpha_1, \cdots, \alpha_s) = \sum_{\mu_0, \mu_1, \cdots, \mu_s} (\mu_0\alpha_0 + \mu_1\alpha_1 + \cdots + \mu_s\alpha_s)^{ut}, \qquad (14)$$

where the $\mu_i$ each run through the $q$ elements of $GF(q)$. Now, let $\alpha_0$ be some linear combination of the $s$ remaining elements

$$\alpha_0 = \lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_s\alpha_s, \qquad (15)$$

and replace $\alpha_0$ by its expression (15) in (14). Then, all terms are linear combinations of the $s$ elements $\alpha_1, \cdots, \alpha_s$, and the $q^s - 1$ terms which do not contain $\alpha_0$ remain invariant, while, among the $(q-1)q^s$ other terms, each one of the $q^s$ distinct linear combinations appears exactly $(q-1)$ times. This is obvious, since we add the fixed elements $\alpha_0, \omega\alpha_0, \cdots, \omega^{q-2}\alpha_0$, to the $q^s$ distinct linear combinations

$$\mu_1\alpha_1 + \mu_2\alpha_2 + \cdots + \mu_s\alpha_s,$$

where the $\mu_i$ each run through the $q$ elements of $GF(q)$. Zero will thus appear $(q-1)$ times, and each one of the $(q^s - 1)$ nonzero linear combinations exactly $q$ times, i.e., zero mod $p$.

### *Lemma 3*

$F_{s,t}(\alpha_0, \alpha_1, \cdots, \alpha_s)$ is zero mod $p$ for all possible choices of $(s+1)$ linearly independent elements $\alpha_0, \alpha_1, \cdots, \alpha_s$, if and only if the multinomial coefficients

$$\frac{(tu)!}{(l_0u)!\,(l_1u)! \cdots (l_su)!} \qquad (16)$$

with $l_i \neq 0$, $l_0 + l_1 + \cdots + l_s = t$, are zero mod $p$.

*Proof*: First, from Lemma 2, if $F_{s,t}$ is zero for all possible choices of linearly independent elements, it is zero for all possible choices. Now, from Lemma 1, $F_{s,t}$ appears to be an homogeneous polynomial of degree $t-1$, less than $v$, in the variables $\alpha_0, \alpha_1, \cdots, \alpha_s$, which has to be zero for all possible choices of the variables, among $v$ elements. This is impossible unless it is identically zero, i.e., unless the multinomial coefficients (16) are zero mod $p$. Theorem 1 then easily follows.

## IV. MAJORITY-LOGIC DECODABLE CYCLIC CODES

The class of cyclic codes to be defined is obtained by taking, for each $C(s, m, p^n)$ previously defined, the dual code $C^*(s, m, p^n)$ over $GF(p)$. This code has block length

$$v = (q^{m+1} - 1)/(q-1)$$

with $q = p^n$, and it has dimension $h$ over $GF(p)$, where $h$ is the number of integers $t$, less than or equal to $v$, $t \neq 0$, such that all multinomial coefficients (16) are congruent to zero mod $p$. A method to calculate this number $h$ is given in Appendix I.

It will be shown that these codes can correctly be decoded using majority logic if not more than $[J/2]$ random errors occurred, where as usual $[x]$ represents the greatest integer not exceeding $x$, and

$$J = (q^{m-s+1} - 1)/(q-1). \qquad (17)$$

### *A. Decoding and Implementation*

The incidence matrix of the $b$ distinct $PG(s, q)$ on the points of a given $PG(m, q)$, which define a balanced incomplete block design with parameters (3), has been taken as a generator matrix for the code $C(s, m, q)$. It can thus be taken as the parity check matrix for $C^*(s, m, q)$.

Now, a given $PG(s-1, q)$ contained in $PG(m, q)$, is contained in exactly $J$ $PG(s, q)$, with $J$ given in (17). On the other hand, the points of $PG(m, q)$ which are not in the given $PG(s-1, q)$ each belong to exactly one $PG(s, q)$ containing the given $PG(s-1, q)$. This is obvious, since the $s$ linearly independent points defining the given $PG(s-1, q)$, together with an additional $(s+1)$th point not in $PG(s-1, q)$, define one and only one $PG(s, q)$. As a consequence, the $J$ parity checks, each of which checks the points of a given $PG(s-1, q)$, form an *orthogonal check set* of order $J$ on these points. Massey[2] defined such a set to consist of a collection of equations, each of which checks a given subset of symbols, with the property that no other symbol appears more than once in the set. Let $e_i$ be the error in the $i$th position, i.e.,

$$e_i = r_i - t_i,$$

where $r_i$ is the $i$th received symbol, and $t_i$ the $i$th transmitted symbol. Then, as shown by Massey,[2] assuming that not more than $[J/2]$ errors occurred, the sum

$$a_j = \sum_{i \in \Gamma_j} e_i, \qquad (18)$$

where $\Gamma_j$ is the set of indices of the points of the $j$th $PG(s-1, q)$, is given correctly as that value of $GF(p)$ which is assumed by the greatest fraction of the $J$ parity checks orthogonal on $\Gamma_j$. Now, the sums $a_j$ (18) may be obtained for each one of the $J$ $PG(s-1, q)$ that are contained in a given $PG(m-1, q)$, and which contain a given $PG(s-2, q)$. These again form an orthogonal check set of order $J$ on the points of the given $PG(s-2, q)$. By induction, one arrives in $s$ steps to an orthogonal check set of order $J$ on a $PG(0, q)$ which contains only one point, thus giving correctly the error $e_j$ in that position as that value of $GF(p)$ assumed by the greatest fraction of the $J$ last checks.

Massey's majority-logic implementation of Meggitt's[10] general decoder can be used to decode these codes. Fig. 1 illustrates a decoder of this type. The $v$ symbols are stored in a buffer storage, while at the same time the syndrome is calculated. The majority element gives as an output the error symbol that was added to the first data symbol by the channel, provided that fewer than $[J/2]$ errors

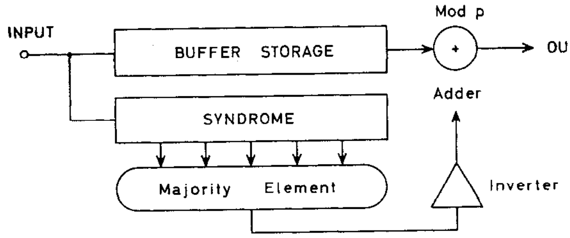

Fig. 1. Meggitt's general decoder.

occurred. All that must be done then is to add the additive inverse of that symbol to the first received symbol, thus correctly giving the first data symbol. Because of the cylic nature of the codes, shifting the registers $v$ times will decode in a sequential manner each one of the $v$ symbols. The majority-logic element has the general structure of an $s$-level tree of majority gates. Each majority gate has $J$ inputs, and its output is that field element which occurs most frequently among its $J$ inputs, provided that it occurs at least $1 + [J/2]$ times; otherwise, it equals zero. Simplifications of this general tree-structure may be obtained in many cases, since, as stated by Massey,[2] the decoding of $v$ symbols needs not more than $v$ majority decisions.

The encoding and syndrome calculations are easily performed because of the cyclic nature of the codes, see, for instance, Peterson.[1]

### *B. General Remarks: Connection with Some Previously Known Codes*

We first remark that, since the code can actually correct up to $[\frac{1}{2}J]$ errors, its minimum distance is at least $J + 1$.

Tables I and II give the parameters for the first few codes over the binary field. Table I is obtained for projective geometries over $GF(2)$; Table II gives the parameters for geometries over $GF(2^2)$ and $GF(2^3)$. $J$, as defined in (21), is the number of parity checks orthogonal on a given $PG(s - 1, q)$; $h$ is the dimension of the code $C^*(s, m, q)$; and $v$, $k$, $b$, $r$, and $\lambda$, are the parameters of the balanced incomplete block design (3), whose incidence matrix is taken as a parity check matrix for the code.

One easily checks that the dimension $h$ of the code $C^*(s, m, 2)$ is given by the sum of the binomial coefficients

$$h = \sum_{i=1}^{s} \binom{m+1}{i}.$$

It may be verified that these codes are equivalent to shortened Reed–Muller codes.[5],[6] On the other hand, the subclass obtained with $m = 2$, $s = 1$ is the class of Weldon's difference-set cyclic codes,[3] for which Graham and MacWilliams[4] proved that

$$v - h = \left[\binom{p+1}{2}\right]^n + 1.$$

TABLE I

$q = 2$

| $m$ | $s$ | $v$ | $k$ | $b$ | $r$ | $\lambda$ | $h$ | $J$ |
|---|---|---|---|---|---|---|---|---|
| 2 | 1 | 7 | 3 | 7 | 3 | 1 | 3 | 3 |
| 3 | 1 | 15 | 3 | 35 | 7 | 1 | 4 | 7 |
|  | 2 | 15 | 7 | 15 | 7 | 3 | 10 | 3 |
| 4 | 1 | 31 | 3 | 155 | 15 | 1 | 5 | 15 |
|  | 2 | 31 | 7 | 155 | 35 | 7 | 15 | 7 |
|  | 3 | 31 | 15 | 31 | 15 | 7 | 25 | 3 |
| 5 | 1 | 63 | 3 | 31.21 | 31 | 1 | 6 | 31 |
|  | 2 | 63 | 7 | 9.31.5 | 31.5 | 15 | 21 | 15 |
|  | 3 | 63 | 15 | 31.21 | 31.5 | 35 | 41 | 7 |
|  | 4 | 63 | 31 | 63 | 31 | 15 | 56 | 3 |
| 6 | 1 | 127 | 3 | 127.21 | 63 | 1 | 7 | 63 |
|  | 2 | 127 | 7 | 127.3.31 | 31.21 | 31 | 28 | 31 |
|  | 3 | 127 | 15 | 127.3.31 | 9.31.5 | 31.5 | 63 | 15 |
|  | 4 | 127 | 31 | 127.21 | 31.21 | 31.5 | 98 | 7 |
|  | 5 | 127 | 63 | 127 | 63 | 31 | 119 | 3 |

TABLE II

| $q$ | $m$ | $s$ | $v$ | $k$ | $h$ | $J$ |
|---|---|---|---|---|---|---|
| 4 | 2 | 1 | 21 | 5 | 11 | 5 |
|  | 3 | 1 | 85 | 5 | 24 | 21 |
|  |  | 2 | 85 | 21 | 68 | 5 |
|  | 4 | 1 | 341 | 5 | 45 | 85 |
|  |  | 2 | 341 | 21 | 195 | 21 |
|  |  | 3 | 341 | 85 | 315 | 5 |
| 8 | 2 | 1 | 73 | 9 | 45 | 9 |
|  | 3 | 1 | 585 | 9 | 184 | 73 |
|  |  | 2 | 585 | 73 | 520 | 9 |

It can be proved that, for the more general class of difference-set codes obtained when $s = m - 1$, one has

$$v - h = \left[\binom{p+s}{p-1}\right]^n + 1.$$

The proof is given in Appendix II. Also, some Bose–Chaudhuri codes fall in this class, such as, for instance, the first six codes of Table I. We note in passing that the fifth code is equivalent to the (31, 15) Bose–Chaudhuri code, but not to the (31, 15) quadratic-residue code, which is known to have the same weight distribution. In fact, for both codes, the dual (31, 16) code contains a balanced incomplete block design with parameters $v = 31$, $k = 7$, $b = 155$, $r = 35$, and $\lambda = 7$; but the first is equivalent to the incidence matrix of the $PG(2, 2)$ on the points of a $PG(4, 2)$, while the other is not.

As a last remark, we note that $\beta^v = 1$ is always a root of the generator polynomial, for the codes $C^*(s, m, q)$, so that, in the binary case, all vectors have even weight. It can be shown that the binary codes of dimensional $h + 1$, obtained by suppressing the root 1, can also be decoded with majority logic, and that their minimum distance is at least $J$ (always odd in the binary case). This result is proved in Appendix III.

## APPENDIX I

For an integer $x$, let $(x)_i$ denote the $i$th "digit," when $x$ is written to the base $p$, i.e.,

$$x = \sum_{i=0}^{\infty} p^i (x)_i, \qquad 0 \leq (x)_i \leq p - 1. \tag{19}$$

The following lemma, the proof of which will be omitted, is a slight extension of a lemma of Graham and MacWilliams[4] (page 1062), and can be proved by a similar argument.

*Lemma 4*

The multinomial coefficient

$$\frac{(a + b + c + \cdots + n)!}{a!\, b!\, c! \cdots n!}$$

is noncongruent to zero mod $p$ if and only if

$$(a)_i + (b)_i + (c)_i + \cdots + (n)_i$$
$$= (a + b + c + \cdots + n)_i \leq p - 1, \; i = 0, 1, 2, \cdots .$$

For an integer $x$, we establish a correspondence with a number $\bar{x}$,

$$\bar{x} = [x]_0 + p[x]_1 + p^2[x]_2 + \cdots + p^{n-1}[x]_{n-1},$$

where $[x]_j$ is defined to be the sum of the "digits" of $x$, whose ranks are congruent to $j$ mod $n$, i.e.,

$$[x]_j = \sum_{k=0}^{\infty} (x)_{kn+j}. \tag{20}$$

One easily verifies that $\bar{x}$ is the sum of the "digits" of $x$, when written to the base $q = p^n$, and that

$$\bar{x} \equiv x \bmod (p^n - 1). \tag{21}$$

We show that the existence of a $(s + 1)$-nomial coefficient (16) noncongruent to zero mod $p$ implies the series of $n$ inequalities

$$\begin{aligned}
\overline{(tu)} &\geq (s + 1)(p^n - 1), \\
\overline{(ptu)} &\geq (s + 1)(p^n - 1), \\
\overline{(p^2tu)} &\geq (s + 1)(p^n - 1), \\
&\vdots \\
\overline{(p^{n-1}tu)} &\geq (s + 1)(p^n - 1).
\end{aligned} \tag{22}$$

For, according to Lemma 4, such a multinomial coefficient (16) exists if and only if

$$(tu)_i = (l_0u)_i + (l_1u)_i + (l_2u)_i + \cdots + (l_su)_i, \qquad i = 0, 1, 2, \cdots ,$$

where $l_ku \not\equiv 0$, and $u = p^n - 1$. These equations imply

$$\overline{(tu)} = \overline{(l_0u)} + \overline{(l_1u)} + \overline{(l_2u)} + \cdots + \overline{(l_su)},$$

with $\overline{(l_ku)} \geq p^n - 1$, see (21), from which the first inequality (22) follows. The other inequalities are easily deduced from

$$(p^itu)_i = (p^il_0u)_i + (p^il_1u)_i + \cdots + (p^il_su)_i$$

by a similar argument. Introducing non-negative integers $a_0, a_1, a_2, \cdots, a_{n-1}$, we can rewrite these relations (22) as

$$\begin{aligned}
&[tu]_0 + p[tu]_1 + p^2[tu]_2 + \cdots + p^{n-1}[tu]_{n-1} \\
&\qquad = (s + 1 + a_0)(p^n - 1), \\
&[tu]_{n-1} + p[tu]_0 + p^2[tu]_1 + \cdots + p^{n-1}[tu]_{n-2} \\
&\qquad = (s + 1 + a_1)(p^n - 1), \\
&\qquad \vdots \\
&[tu]_1 + p[tu]_2 + p^2[tu]_3 + \cdots + p^{n-1}[tu]_0 \\
&\qquad = (s + 1 + a_{n-1})(p^n - 1),
\end{aligned}$$

from which the equivalent relations

$$\begin{aligned}
[tu]_0 &= (s + 1)(p - 1) + a_{n-1}\, p - a_0, \\
[tu]_1 &= (s + 1)(p - 1) + a_{n-2}\, p - a_{n-1}, \\
&\vdots \\
[tu]_{n-1} &= (s + 1)(p - 1) + a_0p - a_1,
\end{aligned} \tag{23}$$

are deduced. By cyclic permutations of the indices, $d_0$ one can always suppose $a_0$ to be the smallest of the $a_j$. Then with

$$b_j = a_j - a_0 \geq 0, \qquad s' = s + a_0,$$

these relations (23) become

$$\begin{aligned}
[tu]_0 &= (s' + 1)(p - 1) + b_{n-1}p \qquad , \\
[tu]_1 &= (s' + 1)(p - 1) + b_{n-2}p - b_{n-1}, \\
&\vdots \\
[tu]_{n-2} &= (s' + 1)(p - 1) + b_1p - b_2, \\
[tu]_{n-1} &= (s' + 1)(p - 1) \qquad\qquad - b_1.
\end{aligned} \tag{24}$$

We now show that, when the relations (24) are satisfied, $s' + 1$ numbers

$$\bar{m}_k = [m_k]_0 + p[m_k]_1 + p^2[m_k]_2 + \cdots + p^{n-1}[m_k]_{n-1},$$

$k = 0, 1, 2, \cdots, s'$, can be found such that

$$\begin{aligned}
&\bar{m}_k = p^n - 1, \\
&[m_0]_j + [m_1]_j + [m_2]_j + \cdots + [m_{s'}]_j = [tu]_j, \\
&\qquad j = 0, 1, 2, \cdots, n - 1.
\end{aligned} \tag{25}$$

For, since the $b_j$ and $[tu]_j$ are non-negative integers, for each $b_j$, $s' + 1$ non-negative integers

$$b_{j,0}, b_{j,1}, b_{j,2}, \cdots, b_{j,s'},$$

the sum of which equals $b_j$, can recursively be found in such a way that the relations

$$b_{0,k} = 0$$

$$b_{j,k} \leq p - 1 + pb_{j-1,k}, \qquad j = 1, 2, \cdots, n-1,$$

$$k = 0, 1, 2, \cdots, s',$$

hold. Then with

$$[m_k]_{n-j} = p - 1 + pb_{j-1,k} - b_{j,k} \geq 0, \tag{26}$$

one easily verifies that the relations (25) are satisfied. It is now a trivial matter to find $(s' + 1)$ numbers

$$m_k = \sum_i (m_k)_i p^i, \qquad 0 \leq (m_k)_i \leq p - 1,$$

such that

$$\sum_i (m_k)_{in+n-j} = [m_k]_{n-j},$$

with $[m_k]_{n-j}$ defined in (26), and

$$\sum_{k=0}^{s'} (m_k)_j = (tu)_j \leq p - 1. \tag{27}$$

Since $m_k \equiv \bar{m}_k = p^n - 1$, mod $p^n - 1$, these numbers $m_k$ are nonzero multiples of $u = p^n - 1$, say $m_k = l_k u$, and from (27), according to Lemma 4, the multinomial coefficients

$$\frac{(tu)!}{(l_0u)!\,(l_1u)! \cdots (l_{s'}u)!},$$

$$\frac{(tu)!}{[(l_0 + l_1)u]!\,(l_2u)! \cdots (l_{s'}u)!}, \text{ etc.} \cdots$$

are noncongruent to zero mod $p$, so that, since $s' \geq s$, certainly a $(s + 1)$-nomial coefficient (16) noncongruent to zero mod $p$ can be found. We have thus proved the following.

*Theorem 2*

The relations (22) are necessary and sufficient conditions for the existence of a $(s + 1)$-nomial coefficient (16) noncongruent to zero mod $p$.

By computing the number of $t$ less than or equal to $v$ and satisfying the conditions of this theorem, one obtains the dimension of the code $C(s, m, q)$ and thus the number of parity symbols of the dual code $C^*(s, m, q)$. The following example illustrates how this computation can be done.

Let $q = 2^2$ and $m = 3$. Then, $u = 3$ and $v = 85$. The integers $t$, $1 \leq t \leq 85$, are divided into classes, each class containing all integers $t$ for which $[tu]_0$ and $[tu]_1$ are the same, i.e., $t_1$ and $t_2$ are in the same class if and only if

$$[t_1u]_0 = [t_2u]_0 \qquad \text{and} \qquad [t_1u]_1 = [t_2u]_1.$$

TABLE III

| $[tu]_0$ | $[tu]_1$ | $N_0$ | $N_1$ | $N$ | $s_m$ |
|---|---|---|---|---|---|
| 1 | 1 | 4 | 4 | 16 | 0 |
| 3 | 0 | 4 | 1 | 4 | 0 |
| 0 | 3 | 1 | 4 | 4 | 0 |
| 2 | 2 | 6 | 6 | 36 | 1 |
| 4 | 1 | 1 | 4 | 4 | 1 |
| 1 | 4 | 4 | 1 | 4 | 1 |
| 3 | 3 | 4 | 4 | 16 | 2 |
| 4 | 4 | 1 | 1 | 1 | 3 |

Let $N_0$, $N_1$ be the number of ways of obtaining $[tu]_0$, $[tu]_1$, respectively, as the sum of $m + 1$ non-negative integers, each of which is less than $p = 2$. Then $N = N_0N_1$ is the number of integers $t$ in the class. To each class, there is attached a number $s_m$, which is the maximum $s$ such that a $(s + 1)$-nomial coefficient (16) noncongruent to zero mod $p$ does exist. According to Theorem 2, $s_m$ is the smallest of the two values $s_0$ and $s_1$, where

$$(s_0 + 1)(p^2 - 1) = [tu]_0 + p[tu]_1,$$

$$(s_1 + 1)(p^2 - 1) = [tu]_1 + p[tu]_0.$$

Table III gives, for each class, the parameters $[tu]_0$ and $[tu]_1$, together with $N_0$, $N_1$, $N$, and $s_m$. One then easily verifies that the codes $C(2, 3, 4)$ and $C(1, 3, 4)$ have respective dimensions 17 and 61; the dual codes thus have dimensions 68 and 24, respectively, as stated in Table II.

## APPENDIX II

Let us prove that, for the general class of difference-set cyclic codes $C^*(m - 1, m, p^n)$, the number of parity symbols is exactly equal to

$$v - h = \left[\binom{m + p - 1}{p - 1}\right]^n + 1.$$

According to Theorems 1 and 2, this number is the number of integers $t$, less than or equal to $v$, $t \neq 0$, such that the relations (22) or equivalently (23), with $s = m - 1$, hold. Since, obviously $[tu]_j \leq (m + 1)(p - 1)$, the only possibilities are

1) $a_0 = a_1 = \cdots = a_{n-1} = 1$, whence $[tu]_0 = [tu]_1 = \cdots = [tu]_{n-1} = (m + 1)(p - 1)$, for which only one corresponding $t$ exists namely $t = v$.

2) $a_0 = a_1 = \cdots = a_{n-1} = 0$, whence $[tu]_0 = [tu]_1 = \cdots = [tu]_{n-1} = m(p - 1)$. Since $[tu]_j$ is the sum of $(m + 1)$ non-negative integers, each of which is less than $p$, the number of ways of obtaining $[tu]_j = m(p - 1)$ is the

same as the number of ways of obtaining $(m + 1 - m)$ $(p - 1)$ as the sum of $(m + 1)$ non-negative integers, i.e. (see [8], 6.6),

$$\binom{p - 1 + m}{m} = \binom{m + p - 1}{p - 1}.$$

There are thus

$$\left[\binom{m + p - 1}{p - 1}\right]^n$$

possibilities in this case. Adding one possibility for the first case, one obtains the announced result.

## APPENDIX III

We now prove that the binary code $(v, h + 1)$ obtained from a given $(v, h)$ code $C^*(s, m, 2^n)$ by suppressing the root $\beta^v = 1$ from its generating polynomial, has minimum distance $J = ((2^n)^{m-s+1} - 1)/(2^n - 1)$, and can be $(s + 1)$-step orthogonalized. For, let $C_1^*$ denote the $(v, h + 1)$ binary code and $C_1$ its dual code, which contains all even-weight vectors of the code $C = C(s, m, 2^n)$, hence the binary sum of any two odd-weight vectors of $C$. Let $p_0, p_1, p_2, \cdots, p_{J-1}$ denote the incidence vectors of the $J$ $PG(s, 2^n)$ containing a given $PG(s - 1, 2^n)$, whose incidence vector we denote by $p_0'$. Since $p_0, p_1, \cdots, p_{J-1}$ form an orthogonal check set on $p_0'$, so do $p_0 + p_1, p_0 + p_2, \cdots, p_0 + p_{J-1}$, each belonging to $C_1$, on $p_0 + p_0'$. But, $p_0 + p_0'$ is the incidence vector of an Euclidean geometry $EG(s, 2^n)$, since the points covered are those of a $PG(s, 2^n)$ which are not in a $PG(s - 1, 2^n)$ contained in it. Thus, $C_1$ contains orthogonal check sets of order $J - 1$ on the points of any $EG(s, 2^n)$ contained in the given $PG(m, 2^n)$. Now, since there are $J$ $EG(s, 2^n)$, each of which is contained in a given $EG(m, 2^n)$ and which contains a given $EG(s - 1, 2^n)$, orthogonal checks sets of order $J - 1$ certainly can be constructed on each $EG(s - 1, 2^n)$. By induction, one arrives in $s + 1$ steps at an orthogonal check set of order $J - 1$ on a single point, hence proving that the code $C_1^*$ can be $(s + 1)$-step orthogonalized; and since each orthogonal check set is of order at least $J - 1$, the minimum distance in $C_1^*$ is at least $J$.

## ACKNOWLEDGMENT

After discovering these codes, the authors became aware of the unpublished, but earlier work of Weldon.[12] In it, a class of binary codes slightly different from theirs is described. Weldon's as well as their results extend and generalize the work of Rudolph,[13] and Kasami, Lin, and Peterson.[14]

## REFERENCES

[1] W. W. Peterson, *Error-Correcting Codes.* Cambridge, Mass.: M.I.T. Press and New York: Wiley, 1961.

[2] J. L. Massey, *Threshold Decoding.* Cambridge, Mass.: M.I.T. Press, 1963.

[3] E. J. Weldon, "Difference-set cyclic codes," *Bell Sys. Tech. J.*, vol. 45, pp. 1045–1055, September 1966.

[4] R. L. Graham and J. MacWilliams, "On the number of information symbols in difference-set cyclic codes," *Bell Sys. Tech. J.*, vol. 45, pp. 1057–1070, September 1966.

[5] I. S. Reed, "A class of multiple-error-correcting codes and the decoding scheme," *IRE Trans. Information Theory*, vol. IT-4, pp. 38–49, September 1954.

[6] D. E. Muller, "Application of Boolean algebra to switching circuit design and to error detection," *IRE Trans. Electronic Computers*, vol. EC-3, pp. 6–12, September 1954.

[7] R. D. Carmichael, *Introduction to the Theory of Groups of Finite Order.* New York: Dover, 1956.

[8] J. Riordan, *An Introduction to Combinatorial Analysis.* New York: Wiley, 1958.

[9] H. B. Mann, *Analysis and Design of Experiments.* New York: Dover, 1949.

[10] J. E. Meggitt, "Error correcting codes and their implementation for data transmission systems," *IRE Trans. Information Theory*, vol. IT-7, pp. 234–244, October 1961.

[11] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error-correcting binary group codes," *Information and Control*, vol. 3, pp. 68–79, March 1960.

[12] E. J. Weldon, "Non-primitive Reed–Muller codes," Dept. of Elec. Engrg., University of Hawaii, Honolulu, December 1966.

[13] L. D. Rudolph, "A class of majority logic decodable codes," *IEEE Trans. Information Theory* (*Correspondence*), vol. IT-13, pp. 305–307, April 1967.

[14] T. Kasami, S. Lin, and W. W. Peterson, "Some results on cyclic codes which are invariant under the affine groups," USAF Cambridge Research Lab., Bedford, Mass., Tech. Rept. AFCRL-66-622, 1966.